

## Выполнение произвольного кода в IBM Lotus Expeditor

**Программа:** IBM Lotus Expeditor 6.1 для Windows.

**Опасность:** Высокая.

**Описание:** Уязвимость существует из-за того, что приложение регистрирует на системе URI обработчик «cai», который позволяет выполнение rcplauncher.exe с произвольными аргументами командной строки. Удаленный пользователь может с помощью специально сформированного аргумента «-launcher» выполнить произвольные команды в системе.

**URL производителя:** [www-306.ibm.com/software/lotus/products/expeditor](http://www-306.ibm.com/software/lotus/products/expeditor).

**Решение:** Установите исправление с сайта производителя.

## Раскрытие данных в Sun Java System Application Server и Web Server

**Программа:** Sun Java System Application Server версии до 7.0.0 2004Q2 R6; Sun Java System Web Server версии до 6.1 SP8; Sun Java System Web Server версии до 7.0 Update 1.

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за неизвестной ошибки, которая позволяет удаленному пользователю просмотреть исходный код JSP-файлов. Подробности уязвимости не сообщаются.

**URL производителя:** [www.sun.com](http://www.sun.com).

**Решение:** Установите исправление с сайта производителя.

## Множественные уязвимости в rdesktop

**Программа:** rdesktop 1.5.0, возможно, более ранние версии.

**Опасность:** Средняя.

**Описание:** 1. Уязвимости существуют из-за потери значимости целочисленных при обработке RDP-запросов в функции iso\_recv\_msg(). Удаленный пользователь может с помощью специально сформированного RDP-запроса вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе с привилегиями пользователя, запустившего rdesktop.

2. Уязвимость существует из-за ошибки в коде, обрабатывающем перенаправляющие RDP-запросы в функции process\_redirect\_pdu(). Удаленный пользователь может с помощью специально сформированного RDP-запроса вызвать переполнение буфера и выполнить произвольный код на целевой системе.

3. Уязвимость существует из-за ошибки при обработке знаковых целочисленных в функции channel\_process(). Удаленный пользователь может вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

Для успешной эксплуатации уязвимостей злоумышленник должен обманом заставить пользователя подключиться к специально сформированному RDP-серверу.

**URL производителя:** [www.rdesktop.org](http://www.rdesktop.org).

**Решение:** Установите исправление с сайта производителя.

## Множественные уязвимости в PHP

**Программа:** PHP-версии до 5.2.6.

**Опасность:** Средняя.

**Описание:** 1. Уязвимость существует из-за неизвестной ошибки в FastCGI SAPI. Удаленный пользователь может вызвать переполнение стека.

2. Уязвимость существует из-за неизвестной ошибки в функциях escapeshellcmd() и escapeshellarg() при обработке неполных многобайтных символов. Удаленный пользователь может обойти ограничения безопасности директив safe\_mode\_exec\_dir и disable\_functions и потенциально выполнить произвольные команды на системе.

3. Уязвимость существует из-за ошибки в механизме трансляции пути в файле cgi\_main.c. Удаленный пользователь может выполнить произвольный код на целевой системе.

4. Уязвимость существует из-за ошибки в cURL. Злоумышленник может обойти ограничения директивы safe\_mode.

5. Уязвимость существует из-за ошибки проверки границ данных в PCRE. Удаленный пользователь может вызвать отказ в обслуживании или скомпрометировать целевую систему.

**URL производителя:** [www.php.net](http://www.php.net).

**Решение:** Установите последнюю версию 5.2.6 с сайта производителя.

## Уязвимость в службе печати в Sun Solaris

**Программа:** Sun Solaris 8, 9, 10.

**Опасность:** Высокая.

**Описание:** Уязвимость существует из-за неизвестной ошибки в службе печати. Удаленный пользователь может вызвать отказ в обслуживании и выполнить произвольный код на целевой системе с привилегиями пользователя root.

**URL производителя:** [www.sun.com](http://www.sun.com).

**Решение:** Установите исправление с сайта производителя.

## Несколько уязвимостей в ядре Linux

**Программа:** Linux kernel 2.6.25.2 и более ранние версии.

**Опасность:** Средняя.

**Описание:** 1. Уязвимость существует из-за отсутствия проверки прав доступа в функции sys\_utimensat(). Локальный пользователь может вызвать отказ в обслуживании.

2. Уязвимость существует из-за утечки памяти в функции «iprip6\_rcv()», входящей в состав тоннельного драйвера IPv6 over IPv4 (SIP). Удаленный пользователь может с помощью специально сформированного сетевого пакета потребить все доступные системные ресурсы.

**URL производителя:** [www.kernel.org](http://www.kernel.org).

**Решение:** Установите последнюю версию ядра 2.6.25.3 с сайта производителя.

Составил Александр Антипов